REMARKS

By this Amendment, Applicants amend claims 2, 6, and 11. Claims 2-19 are currently pending.

In the final Office Action, the Examiner allowed claim 19. The Examiner rejected claims 11-18 under 35 U.S.C. § 112, first paragraph, as failing to comply with the written description requirement; and rejected claims 11-18 under 35 U.S.C. § 112, second paragraph, as indefinite. The Examiner also rejected claims 2-4, 6, 7, and 9 under 35 U.S.C. § 102(e) as anticipated by U.S. Patent No. 6,397,241 to Glaser et al. ("Glaser"); rejected claims 5 and 10 under 35 U.S.C. § 103(a) as unpatentable over Glaser; rejected claim 8 under 35 U.S.C. § 103(a) as unpatentable over Glaser in view of Becker, 4-bit Multiplier using Mentor Graphics, Student Lab-Report for Course BEng 2, University of East London (August 12, 1998) ("Becker"); rejected claims 11, 17, and 18 under 35 U.S.C. § 103(a) as unpatentable over U.S. Patent No. 6,230,179 to Dworkin et al. (hereinafter "Dworkin") in view of Drescher et al., VLSI Architectures for Multiplication in GF(2^m) for Application Tailored Digital Signal Processors (1997) ("Drescher"); rejected claim 12 under 35 U.S.C. § 103(a) as unpatentable over Dworkin in view of Drescher and in further view of U.S. Patent No. 4,692,888 to New ("New"); rejected claim 13 under 35 U.S.C. § 103(a) as unpatentable over Dworkin in view of Drescher and New and in further view of U.S. Patent No. 3,064,896 to Carroll et al. ("Carroll"); and rejected claims 14 and 15 under 35 U.S.C. § 103(a) as unpatentable over Dworkin in view of Drescher, New, and Carroll, and in further view of U.S. Patent No. 5,468,297

to Zook ("Zook").[1] Applicants respectfully traverse the Examiner's rejections under § 102, § 103, and § 112.

Regarding the Rejections Under 35 U.S.C. § 112

Applicants respectfully traverse the Examiner's rejection of claims 11-18 under 35 U.S.C. § 112, first paragraph, as failing to comply with the written description requirement; and rejection of claims 11-18 under 35 U.S.C. § 112, second paragraph, as indefinite. The Examiner alleged that "[t]he specification does not explicitly disclose a long product-sum operation circuit which executes only polynomial multiplication with a finite field $GF(2^m)$ based polynomial base expression," and "'polynomial multiply processing' is an action and 'a modulo' is a number; therefore it is unclear whether the divide is separating processes or is dividing a value." (Office Action at 4-5.) Applicants respectfully disagree. However, to expedite the prosecution of this application, Applicants have amended independent claim 11 such that claim 11 recites "modulo processing" and does not recite "executes only polynomial multiplication." Accordingly, Applicants respectfully request withdrawal of the Section 112 rejection of claims 11-18.

Regarding the Rejections Under 35 U.S.C. § 102

Applicants respectfully traverse the Examiner's rejection of claims 2-4, 6, 7, and 9 under 35 U.S.C. § 102(e) as anticipated by Glaser. In order to anticipate Applicants' claimed invention under 35 U.S.C. § 102, each and every element of the claim in issue must be found, either expressly described or under principles of inherency, in a single prior art reference. Further, "[t]he identical invention must be shown in as complete

[1] The Office Action contains a number of statements reflecting characterizations of the related art and the claims. Regardless of whether any such statement is identified herein, Applicants decline to automatically subscribe to any statement or characterization in the Office Action.

detail as is contained in the . . . claim." See M.P.E.P. § 2131, quoting Richardson v. Suzuki Motor Co., 868 F.2d 1126, 1236, 9 U.S.P.Q.2d 1913, 1920 (Fed. Cir. 1989).

Independent claim 2, as amended, recites a combination including, for example, "an adder circuit shared by the separated integer based multiplier circuit and the finite field GF(2^m)-based circuit and configured to operate on data from either the integer based multiplier circuit or the finite field GF(2^m)-based circuit." Glaser fails to disclose at least the claim element listed above as recited in amended claim 2.

The Examiner alleged that "Glaser discloses an arithmetic apparatus/integrated cryptographic circuit incorporated in a LSI/smartcard (col. 2, lines 1-10) for performing a long integer product-sum arithmetic operation (col. 3, lines 20-33), the arithmetic apparatus/integrated cryptographic circuit comprising an integer based unit arithmetic circuit/RSA arithmetic processor (Fig. 1, #18), a finite field GF(2^m) based unit arithmetic circuit/ECC arithmetic processor logically adjacent to said integer based unit arithmetic circuit (Fig. 1, #20 & col. 1, lines 9-21), and a selector/control configured to select one of said integer unit arithmetic circuit/RSA and said finite field GF(2^m) based unit arithmetic circuit/ECC." (Office Action at 5). Applicants respectfully disagree. However, even assuming that Glaser discloses what the Examiner alleged, Glaser fails to disclose at least "an adder circuit shared by the separated integer based multiplier circuit and the finite field GF(2^m)-based circuit and configured to operate on data from either the integer based multiplier circuit or the finite field GF(2^m)-based circuit," as recited in amended claim 2 (emphasis added).

Therefore, Glaser fails to disclose each and very element of amended claim 2. Glaser thus cannot anticipate claim 2 under 35 U.S.C. § 102. Accordingly, Applicants

respectfully request withdrawal of the Section 102 rejection of claim 2. Because claims 3 and 4 depend from claim 2, Applicants also request withdrawal of the Section 102 rejection of claims 3 and 4 for at least the same reasons stated above.

Independent claim 6, as amended, recites a combination including, for example, "wherein the arithmetic circuit comprises a full adder, the full adder including a carry propagation section configured to propagate a carry of an operation result of the full adder upon reception of a selection signal corresponding to an integer-based unit arithmetic operation and to not propagate the carry of the full adder upon reception of a selection signal corresponding to a finite field $GF(2^m)$-based unit arithmetic operation." Glaser fails to disclose at least the claim elements listed above as recited in amended claim 6.

The Examiner alleged that Glaser discloses "a carry propagation controller (Fig. 1, #16) configured to propagate, when a long product-sum operation is to be executed, a carry of an operation result obtained by said integer based unit arithmetic circuit upon reception of a selection signal corresponding to an integer based unit arithmetic operation, and a propagate no carry of the operation result upon reception of a selection signal corresponding to a finite field GF(2^m) based unit arithmetic operation (col. 5, lines 1-6), wherein an integer based multiply operation and a finite field GF(2^m) based multiply operation is switched by controlling the carry propagation (col. 5, lines 1-6)." (Office Action at 6). Applicants respectfully disagree.

However, even assuming that Glaser discloses what the Examiner alleged, Glaser fails to disclose at least "wherein the arithmetic circuit comprises a full adder, the full adder including a carry propagation section configured to propagate a carry of an

operation result of the full adder upon reception of a selection signal corresponding to an integer-based unit arithmetic operation and to not propagate the carry of the full adder upon reception of a selection signal corresponding to a finite field GF(2^m)-based unit arithmetic operation," as recited in amended claim 6 (emphasis added).

Therefore, Glaser fails to disclose each and very element of amended claim 6. Glaser thus cannot anticipate claim 6 under 35 U.S.C. § 102. Accordingly, Applicants respectfully request withdrawal of the Section 102 rejection of claim 6. Because claims 7 and 9 depend from claim 2, Applicants also request withdrawal of the Section 102 rejection of claims 7 and 9 for at least the same reasons stated above.

Regarding the Rejections Under 35 U.S.C. § 103

Applicants respectfully traverse the Examiner's rejection of claims 5 and 10 under 35 U.S.C. § 103(a) as unpatentable over Glaser. In order to establish a *prima facie* case of obviousness, three basic criteria must be met. First, the prior art reference (or references when combined) must teach or suggest all the claim elements. Second, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify a reference or to combine reference teachings. Third, there must be a reasonable expectation of success. See M.P.E.P. § 2143.

Claims 5 and 10 depend from claims 2 and 6, respectively. As set forth above, Glaser fails to teach or suggest at least "an adder circuit shared by the separated integer based multiplier circuit and the finite field GF(2^m)-based circuit and configured to operate on data from either the integer based multiplier circuit or the finite field GF(2^m)-based circuit," as recited in claim 2 and required by claim 5, and also fails to teach or

suggest at least "wherein the arithmetic circuit comprises a full adder, the full adder including a carry propagation section configured to propagate a carry of an operation result of the full adder upon reception of a selection signal corresponding to an integer-based unit arithmetic operation and to not propagate the carry of the full adder upon reception of a selection signal corresponding to a finite field GF(2^m)-based unit arithmetic operation," as recited in claim 6 and required by claim 10.

Therefore, Glaser fails to teach or suggest all claim elements required by claims 5 and 10. A *prima facie* case of obviousness has not been established. Accordingly, Applicants respectfully request withdrawal of the Section 103 rejection of claims 5 and 10.

Applicants also respectfully traverse the Examiner's rejection of claim 8 under 35 U.S.C. § 103(a) as unpatentable over Glaser in view of Becker. Claim 8 depends from claim 6. As set forth above, Glaser fails to teach or suggest at least "wherein the arithmetic circuit comprises a full adder, which further includes a carry propagation section configured to propagate a carry of an operation result of the full adder upon reception of a selection signal corresponding to an integer-based unit arithmetic operation, and not propagate the carry of the full adder upon reception of a selection signal corresponding to a finite field GF(2^m)-based unit arithmetic operation," as recited in claim 6 and required by claim 8.

Becker fails to cure Glaser's deficiencies. Even assuming that Becker teaches "a full adder works in such a way that the carry is XOR'ed with the partial sum to produce the output (page 4, §4)," which Applicants do not necessarily agree, Becker's teaching of XOR'ed carry does not constitute "wherein the arithmetic circuit comprises a full

adder, the full adder including a carry propagation section configured to propagate a carry of an operation result of the full adder upon reception of a selection signal corresponding to an integer-based unit arithmetic operation and to not propagate the carry of the full adder upon reception of a selection signal corresponding to a finite field GF(2^m)-based unit arithmetic operation," as recited in claim 6 and required by claim 8 (emphasis added).

Therefore, neither Glaser nor Becker, taken alone or in any reasonable combination, teaches or suggest all the elements required by claim 8. A *prima facie* case of obviousness has not been established. Accordingly, Applicants respectfully request withdrawal of the Section 103 rejection of claim 8.

Applicants also respectfully traverse the Examiner's rejection of claims 11, 17, and 18 under 35 U.S.C. § 103(a) as unpatentable over Dworkin in view of Drescher. Independent claim 11, as amended, recites a combination including, for example, "a controller module configured to divide the processing of modular multiplication of the integer unit arithmetic operation and the finite field GF(2^m)-based unit arithmetic operation into polynomial multiply processing and modulo processing and to cause the integer unit arithmetic circuit to execute the polynomial multiply processing; wherein the controller module selects the one of an integer unit arithmetic operation and finite field GF(2^m)-based unit arithmetic operation and executes the modulo processing on the integer unit arithmetic circuit." Dworkin fails to teach or suggest at least the claim elements listed above as recited in claim 11.

Dworkin discloses "[a] finite field multiplier with intrinsic modular reduction [that] includes an interface unit (1208) that translates an n bit wide data path to a m bit wide

data path where n is less than m." Dworkin, abstract, emphasis added. However, Dworkin fails to teach or suggest at least "a controller module configured to divide the processing of modular multiplication of the integer unit arithmetic operation and the finite field GF(2^m)-based unit arithmetic operation into polynomial multiply processing and modulo processing and to cause the integer unit arithmetic circuit to execute the polynomial multiply processing; wherein the controller module selects the one of an integer unit arithmetic operation and finite field GF(2^m)-based unit arithmetic operation and executes the modulo processing on the integer unit arithmetic circuit," as recited in claim 11 (emphasis added).

The Examiner alleged that "Dworkin discloses . . . a controller module/controller (Fig. 1, #20) configured to divide the modular multiplication into polynomial multiply processing and a modulo (col. 5, lines 1-10)." (Office Action at 9). Applicants respectfully disagree.

Dworkin, in column 5, lines 1-10, discloses that "[i]t may be seen that this signal implements the modular reduction of the partial product in the accumulator C by the modulus vector m, when the topmost bit C_m of C is set." Dworkin, column 5, lines 4-6. However, Dworkin's finite field multiplication uses interweaving, or undivided, processing of partial product followed by intrinsic modular reduction, which does not constitute "a controller module configured to divide the processing of modular multiplication of the integer unit arithmetic operation and the finite field GF(2^m)-based unit arithmetic operation into polynomial multiply processing and modulo processing and to cause the integer unit arithmetic circuit to execute the polynomial multiply processing; wherein the controller module selects the one of an integer unit arithmetic operation and

finite field GF(2^m)-based unit arithmetic operation and executes the modulo processing on the integer unit arithmetic circuit," as recited in claim 11 (emphasis added).

Drescher fails to cure Dworkin's deficiencies. Drescher merely discloses "a new multiplier architecture that performs both types of multiplications employing the same logical cells with a low complexity and a marginal propagation overhead." Drescher, section 4.1. However, Drescher fails to mention at least "divide the processing of modular multiplication of the integer unit arithmetic operation and the finite field GF(2^m)-based unit arithmetic operation," as recited in claim 11.

Therefore, neither Dworkin nor Drescher, taken alone or in any reasonable combination, teaches or suggest all the elements required by claim 11. A *prima facie* case of obviousness has not been established. Accordingly, Applicants respectfully request withdrawal of the Section 103 rejection of claim 11. Because claims 17 and 18 depend from claim 11, Applicants also request withdrawal of the Section 103 rejection of claims 17 and 18 for at least as being dependent from allowable base claim 11.

Applicants also respectfully traverse the Examiner's rejection of claim 12 under 35 U.S.C. § 103(a) as unpatentable over Dworkin in view of Drescher and in further view of New. Claim 12 depends from claim 11.

As explained above, Dworkin and Drescher fail to teach or suggest at least "a controller module configured to divide the processing of modular multiplication of the integer unit arithmetic operation and the finite field GF(2^m)-based unit arithmetic operation into polynomial multiply processing and modulo processing and to cause the integer unit arithmetic circuit to execute the polynomial multiply processing; wherein the controller module selects the one of an integer unit arithmetic operation and finite field

GF(2^m)-based unit arithmetic operation and executes the modulo processing on the integer unit arithmetic circuit," as recited in claim 11 and required by claim 12.

Further, even assuming that "New teaches an internal method of product-sum formation (col. 2, liens 1-12)," (Office Action at 10), which Applicants do not necessarily agree, New fails to teach or suggest at least "a controller module configured to divide the processing of modular multiplication of the integer unit arithmetic operation and the finite field GF(2^m)-based unit arithmetic operation into polynomial multiply processing and modulo processing and to cause the integer unit arithmetic circuit to execute the polynomial multiply processing; wherein the controller module selects the one of an integer unit arithmetic operation and finite field GF(2^m)-based unit arithmetic operation and executes the modulo processing on the integer unit arithmetic circuit," as recited in claim 11 and required by claim 12 (emphasis added).

Therefore, none of Dworkin, Drescher, and New teaches or suggest all elements required by claim 12. A *prima facie* case of obviousness has not been established. Accordingly, Applicants respectfully request withdrawal of the Section 103 rejection of claim 12.

Applicants also respectfully traverse the Examiner's rejection of claim 13 under 35 U.S.C. § 103(a) as unpatentable over Dworkin in view of Drescher and New and in further view of Carroll. Claim 13 depends from claim 11 indirectly.

As set forth above, Dworkin, Drescher, and New fail to teach or suggest at least "a controller module configured to divide the processing of modular multiplication of the integer unit arithmetic operation and the finite field GF(2^m)-based unit arithmetic operation into polynomial multiply processing and modulo processing and to cause the

integer unit arithmetic circuit to execute the polynomial multiply processing; wherein the controller module selects the one of an integer unit arithmetic operation and finite field GF(2^m)-based unit arithmetic operation and executes the modulo processing on the integer unit arithmetic circuit," as recited in claim 11 and required by claim 13.

Further, even assuming that "Carroll teaches a method, and accompanying apparatus for division that allows adequate time for the maximum number of carries and eliminates unnecessary processing (col. 2, lines 1-35)," (Office Action at 11), which Applicants do not necessarily agree, Carroll fails to teach or suggest at least "a controller module configured to divide the processing of modular multiplication of the integer unit arithmetic operation and the finite field GF(2^m)-based unit arithmetic operation into polynomial multiply processing and modulo processing and to cause the integer unit arithmetic circuit to execute the polynomial multiply processing; wherein the controller module selects the one of an integer unit arithmetic operation and finite field GF(2^m)-based unit arithmetic operation and executes the modulo processing on the integer unit arithmetic circuit," as recited in claim 11 and required by claim 13 (emphasis added).

Therefore, none of Dworkin, Drescher, New, and Carroll teaches or suggest all elements required by claim 13. A *prima facie* case of obviousness has not been established. Accordingly, Applicants respectfully request withdrawal of the Section 103 rejection of claim 13.

Applicants also respectfully traverse the Examiner's rejection of claims 14 and 15 under 35 U.S.C. § 103(a) as unpatentable over Dworkin in view of Drescher, New, Carroll, and Zook. Claims 14 and 15 depend from claim 11 indirectly.

As set forth above, Dworkin, Drescher, New, and Carroll fail to teach or suggest at least "a controller module configured to divide the processing of modular multiplication of the integer unit arithmetic operation and the finite field GF(2^m)-based unit arithmetic operation into polynomial multiply processing and modulo processing and to cause the integer unit arithmetic circuit to execute the polynomial multiply processing; wherein the controller module selects the one of an integer unit arithmetic operation and finite field GF(2^m)-based unit arithmetic operation and executes the modulo processing on the integer unit arithmetic circuit," as recited in claim 11 and required by claims 14 and 15.

Further, even assuming that "Zook teaches that division is a very complex operation in finite field arithmetic, as compared to multiplication," as asserted by the Examiner, (Office Action at 11), which Applicants do not necessarily agree, Zook fails to teach or suggest at least "a controller module configured to divide the processing of modular multiplication of the integer unit arithmetic operation and the finite field GF(2^m)-based unit arithmetic operation into polynomial multiply processing and modulo processing and to cause the integer unit arithmetic circuit to execute the polynomial multiply processing; wherein the controller module selects the one of an integer unit arithmetic operation and finite field GF(2^m)-based unit arithmetic operation and executes the modulo processing on the integer unit arithmetic circuit," as recited in claim 11 and required by claims 14 and 15 (emphasis added).

Therefore, none of Dworkin, Drescher, New, Carroll, and Zook teaches or suggest all elements required by claims 14 and 15. A *prima facie* case of obviousness

has not been established. Accordingly, Applicants respectfully request withdrawal of the Section 103 rejection of claims 14 and 15.

Conclusion

In view of the foregoing amendments and remarks, Applicants respectfully request reconsideration and reexamination of this application and the timely allowance of the pending claims.

Please grant any extensions of time required to enter this response and charge any additional required fees to our deposit account 06-0916.

Respectfully submitted,

FINNEGAN, HENDERSON, FARABOW,
GARRETT & DUNNER, L.L.P.

Dated: January 25, 2006

By: Wenye
Wenye Tan
Reg. No. 55,662